Draft for Public Comment

Form 36

DPC: 21/30446697 DC

BSI Group Headquarters

389 Chiswick High Road London W4 4AL

Tel: +44 (0)20 8996 9000
Fax: +44 (0)20 8996 7400
www.bsigroup.com

Date: 05 November 2021
Origin: International

Latest date for receipt of comments: 29 December 2021

Project No. 2019/03351

Responsible committee: TCT/7 Telecommunications - Installation requirements

Interested committees:

Title: Draft BS ISO/IEC 24383 Information technology - Physical network security for the accommodation of customer premises cabling infrastructure and information technology equipment.

Please notify the secretary if you are aware of any keywords that might assist in classifying or identifying the standard or if the content of this standard

i) has any issues related to 3rd party IPR, patent or copyright
ii) affects other national standard(s)
iii) requires additional national guidance or information

WARNING: THIS IS A DRAFT AND MUST NOT BE REGARDED OR USED AS A BRITISH STANDARD. THIS DRAFT IS NOT CURRENT BEYOND 29 December 2021

This draft is issued to allow comments from interested parties; all comments will be given consideration prior to publication. No acknowledgement will normally be sent. **See overleaf for information on the submission of comments.**

No copying is allowed, in any form, without prior written permission from BSI except as permitted under the Copyright, Designs and Patent Act 1988 or for circulation within a nominating organization for briefing purposes. Electronic circulation is limited to dissemination by e-mail within such an organization by committee members.

Further copies of this draft may be purchased from BSI Shop http://shop.bsigroup.com or from BSI Customer Services, Tel: +44(0) 20 8996 9001 or email cservices@bsigroup.com. British, International and foreign standards are also available from BSI Customer Services.

Information on the co-operating organizations represented on the committees referenced above may be obtained from https://standardsdevelopment.bsigroup.com/.

Responsible Committee Secretary: Ms Joy Tan (BSI)
Direct tel:
E-mail: joy.tan@bsigroup.com

Documents
Document Sharing Hub
Full document details: 21/30446697 DC

Introduction

This draft standard is based on national and international discussions. Your comments on this draft are invited and will assist in the preparation of the consequent standard.

For international standards, comments will be reviewed by the relevant UK national committee before sending the consensus UK vote and comments to the international committee, which will then decide appropriate action. If the international standard is approved, it is usual for the text to be published as a British Standard.

For national standards, comments will be reviewed by the relevant UK national committee and the resulting standards published as a British Standard.

UK Vote

Please indicate whether you consider the UK should submit a negative (with supporting technical reasons) or positive vote on this draft. Please indicate if you are aware of any reason why this draft standard should not be published as a British Standard.

Submission of Comments

- **Annotated drafts are not acceptable and will be rejected.**
- All comments should be submitted online at **https://standardsdevelopment.bsigroup.com/**. You will need to register in order to comment.

Template for comments and secretariat observations

Date: xx/xx/20xx	Document: ISO/DIS xxxx

1	2	(3)	4	5	(6)	7
MB	Clause No./ Subclause No./Annex **(e.g. 3.1)**	Paragraph/Figure/ Table/Note	**Type of comment**	**Commend (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations on each comment submitted**
	3.1	Definition 1	ed	Definition is ambiguous and needs clarifying.	Amend to read '...so that the mains connector to which no connection...'	
	6.4	Paragraph 2	te	The use of the UV photometer as an alternative cannot be supported as serious problems have been encountered in its use in the UK.	Delete reference to UV photometer.	

Documents
Document Sharing Hub

Full document details: 21/30446697 DC

JTC1-SC25/3069/CD

COMMITTEE DRAFT (CD)

PROJECT NUMBER: **ISO/IEC 24383 ED1**	
DATE OF CIRCULATION: **2021-11-05**	CLOSING DATE FOR COMMENTS: **2022-01-28**
SUPERSEDES DOCUMENTS: **JTC1-SC25/3022/CD, JTC1-SC25/3049A/CC**	

IEC ISO/IEC JTC 1/SC 25 : INTERCONNECTION OF INFORMATION TECHNOLOGY EQUIPMENT	
SECRETARIAT: Germany	SECRETARY: Mr Marco Peter
OF INTEREST TO THE FOLLOWING COMMITTEES:	PROPOSED HORIZONTAL STANDARD: ☐ Other TC/SCs are requested to indicate their interest, if any, in this CD to the secretary.
FUNCTIONS CONCERNED: ☐ EMC ☐ ENVIRONMENT ☐ QUALITY ASSURANCE ☐ SAFETY	

This document is still under study and subject to change. It should not be used for reference purposes.

Recipients of this document are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

TITLE:

Information technology - Physical network security for the accommodation of customer premises cabling infrastructure and information technology equipment

NOTE FROM TC/SC OFFICERS:

Copyright © 2021 International Electrotechnical Commission, IEC. All rights reserved. It is permitted to download this electronic file, to make a copy and to print out the content for the sole purpose of preparing National Committee positions. You may not copy or "mirror" the file or printed version of the document, or any part of it, for any other purpose without permission in writing from IEC.

AVA Documents Document Sharing Hub

Full document details: 21/30446697 DC

CONTENTS

FOREWORD 5
INTRODUCTION 6
1 Scope 7
2 Normative references 7
3 Definitions and abbreviations 8
3.1 Definitions 8
3.2 Abbreviations 10
4 Conformance 10
5 Principles 11
5.1 General 11
5.2 Relationship with ISO/IEC 27000 series 11
5.3 Risk assessment concepts 11
5.4 Defence in depth 12
5.5 Network infrastructure 15
5.6 Controlling access 15
5.7 Perimeters and spaces 15
5.8 Threat 19
6 Public perimeter 19
6.1 Spaces and structures 19
6.2 Pathways 20
6.3 Infrastructure components 21
7 Building perimeter 22
7.1 Spaces and structures 22
7.2 Pathways 27
7.3 Infrastructure components 28
8 Equipment/distributor room 29
8.1 Spaces and structures 29
8.2 Pathways 35
8.3 Infrastructure components 36
9 Rack/cabinet 37
9.1 Spaces and structures 37
9.2 Pathways 39
9.3 Infrastructure components 40
10 Cabling component containment 43
10.1 Spaces and structures 43
10.2 Pathways 44
10.3 Infrastructure components 49
11 Cabling component 49
11.1 Spaces and structures 49
11.2 Pathways 50
11.3 Infrastructure components 51
12 Administration 54
12.1 Reporting of cyber security incidents 54
12.2 Labelling 54

AVA Documents
Document Sharing Hub

Full document details: 21/30446697 DC

12.3 Documentation 55
12.4 Cable inspections 55
12.5 Monitor the system 56
12.6 Security documentation....56
12.7 Security assessment report....57
12.8 Training....57
12.9 Security clearances 57
12.10 Access requirements 57
13 Evolution of security systems 57
Annex A (normative) Free standing barriers 59
Annex B (informative) Video surveillance 60
B.1 Requirements 60
B.1.1 Cabling, pathways and spaces 60
B.1.2 Cameras 60
B.1.3 Monitoring 60
B.2 Recommendations 60
B.2.1 Pathways 60
B.2.2 Cameras 60
B.2.3 Monitoring....61
B.2.4 Security lighting 61
Annex C (informative) Intrusion detection....62
C.1 Requirements 62
C.1.1 Cabling, pathways and spaces 62
C.1.2 Deployment....62
C.1.3 Monitoring 63
C.1.4 Documentation 63
C.1.5 Operation....63
Annex D (informative) Access control....64
D.1 Requirements 64
D.1.1 Cabling, pathways and spaces 64
D.1.2 Deployment....64
D.2 Recommendations 65
D.2.1 Planning....65
D.2.2 Pathways 65
Annex E (informative) Management of personnel....66
E.1 Requirements 66
E.1.1 Employees and other authorized personnel 66
E.1.2 Manned guarding....66
E.1.3 Visitors....67
E.1.4 Deliveries....67
E.2 Recommendations 67
E.2.1 Visitors....67
E.2.2 Deliveries....67
Bibliography....68

Documents
Document Sharing Hub
Full document details: 21/30446697 DC

List of figures

Figure 1 – Risk assessment concepts 11
Figure 2 – Defence in depth model 13
Figure 3 – Area and room relationship – solution one 16
Figure 4 – Area and room relationship – solution two 17
Figure 5 – Area and room relationship – solution three 18
Figure 6 – Example of single steel panel (internal) wall construction. 24
Figure 7 – Example of dual steel panel (internal) wall construction 25
Figure 8 – Security requirements for an ‘open’ equipment/distributor room. 30
Figure 9 – Security requirements for an ‘restricted’ equipment room. 31
Figure 10 – Security requirements for an ‘secure’ equipment room. 32
Figure 11 – Security requirements for an ‘highly secure’ equipment room. 33
Figure 12 – Security requirements for an ‘highly secure’ equipment room in a lower classified area 34
Figure 13 – Example of various classifications of cable reticulation between equipment racks 42
Figure 14 – Optical fibre security conduit application 45
Figure 15 – Examples of access pit security configuration 47
Figure A.1 – Examples of free-standing barriers and minimum effective heights 59

List of tables

Table 1 – Equipment room classification and minimum area classification 14
Table 2 – Recommended cabinet grouping for patch panels 40
Table 3 – Minimum acceptable classification combinations for cables for reticulation systems. 44
Table 4 – Classification security seal minimum requirements. 47
Table 5 – Example of classification cable colour 52
Table 6 – Example of telecommunications outlet wall boxes. 53
Table 7 – Maximum period between cable inspections 55

Documents
Document Sharing Hub
Full document details: 21/30446697 DC

INFORMATION TECHNOLOGY –
Generic cabling – Physical network security for the accommodation of customer premises cabling infrastructure and information technology equipment

FOREWORD

1) ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

2) The formal decisions or agreements of IEC and ISO on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees and ISO member bodies.

3) IEC, ISO and ISO/IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees and ISO member bodies in that sense. While all reasonable efforts are made to ensure that the technical content of IEC, ISO and ISO/IEC publications is accurate, IEC or ISO cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.

4) In order to promote international uniformity, IEC National Committees and ISO member bodies undertake to apply IEC, ISO and ISO/IEC publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any ISO, IEC or ISO/IEC publication and the corresponding national or regional publication should be clearly indicated in the latter.

5) ISO and IEC do not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. ISO or IEC are not responsible for any services carried out by independent certification bodies.

6) All users should ensure that they have the latest edition of this publication.

7) No liability shall attach to IEC or ISO or its directors, employees, servants or agents including individual experts and members of their technical committees and IEC National Committees or ISO member bodies for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication of, use of, or reliance upon, this ISO/IEC Publication or any other IEC, ISO or ISO/IEC publications.

8) Attention is drawn to the normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.

9) Attention is drawn to the possibility that some of the elements of this ISO/IEC Publication may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

International Standard ISO/IEC 24383 was prepared by subcommittee 25: Interconnection of information technology equipment, of ISO/IEC joint technical committee 1: Information technology.

This International Standard has been approved by vote of the member bodies, and the voting results can be obtained from the address given on the second title page.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

Documents
Document Sharing Hub

Full document details: 21/30446697 DC

INTRODUCTION

ISO/IEC 14763-2 specifies requirements and recommendations for the installation specification, quality assurance and installation practices for customer premises cabling in accordance with the ISO/IEC 11801 series.

Those requirements provide basic level of physical network security for the cabling and associated infrastructure.

This document builds upon the requirements of ISO/IEC 14763-2 by facilitating the timely and effective protection of the customer premises cabling infrastructure to avoid loss/damage to the physical information transport network and therefore supports the protection of the transmitted information.

This document provides comprehensive planning and installation requirements for improving physical network security.

The requirements and recommendations can be applied to existing buildings and also during building construction, or renovation, when actions are significantly less expensive and less disruptive than after the building is occupied.

This document incorporates the use of automated infrastructure management (AIM) systems, including those in accordance with ISO/IEC 18598, to further enhance the security of cabling infrastructure and integrate the physical network security with other security systems in the premises.

This document is intended to be used by

- architects, building owners, building designers and builders,
- consultants,
- facility managers and network managers,
- designers, suppliers, installers, inspectors (auditors), maintainers and owners of telecommunications cabling.

When using this standard, it must be considered relevant specifications from ISO/IEC 27000 series.

Documents
Document Sharing Hub

Full document details: 21/30446697 DC

INFORMATION TECHNOLOGY - Generic cabling – Physical network security for the accommodation of customer premises cabling infrastructure and information technology equipment

1 Scope

This document specifies requirements and recommendations providing security to the physical network comprising customer premises cabling in accordance with ISO/IEC 11801 series, associated infrastructure and accommodation of information technology equipment.

The document covers the security of the telecommunications cables, pathways, spaces, and other infrastructure components of the telecommunications physical infrastructure to protect the telecommunications infrastructure from theft, vandalism, intrusions, and unauthorized modifications.

The document addresses

a) risk assessment guidelines,
b) design (including construction), planning and installation practices based on a required information sensitivity level,
c) intrusion detection,
d) administration including Automated Infrastructure Management (AIM).

This document applies to existing buildings and structures together with those being planned for construction.

The following are outside the scope of this document:

1) data protection methods such as encryption,
2) practices that address protection from non-contact cable tapping, audio, visual or RF snooping and other forms of unauthorized monitoring.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 60839 *Alarm and electronic security systems*

IEC 60839-11-1 *Alarm and electronic security systems - Part 11-1: Electronic access control systems - System and components requirements*

IEC 62676 *Video Surveillance Systems for use in security applications*

IEC 62676-1-1:2013, *Video surveillance systems for use in security applications Part 1-1: System requirements – General*

ISO 31000 *Risk management*

ISO/IEC 11801 *Information technology — Generic cabling for customer premises*

ISO/IEC 14763-2, *Information technology - Implementation and operation of customer premises cabling - Part 2: Planning and installation*

ISO/IEC 27000 *Information security management systems*

Documents
Document Sharing Hub

Full document details: 21/30446697 DC

3 Definitions and abbreviations

3.1 Definitions

For the purposes of this document the terms and definitions of ISO/IEC 14763-2 and the following apply.

3.1.1
access control system
system that provides selective restriction of access to a space or cabling component

3.1.2
administration
methodology defining the documentation requirements of a cabling system and its containment, the labelling of functional elements and the process by which moves, additions and changes are recorded
[SOURCE: ISO/IEC 11801-1:2017, 3.1.1]

3.1.3
AIM system
integrated hardware and software system that automatically detects the insertion or removal of cords, documents the cabling infrastructure including connected equipment enabling management of the infrastructure and data exchange with other systems
[SOURCE: ISO/IEC 18598:2016, 3.1.3]

3.1.4
alarmed carrier
system for detecting intrusion into a pathway using optical fibre as a vibration sensor

3.1.5
alarm-enabled
capable of triggering an alarm with the intrusion alarm system

3.1.6
authorized personnel
persons able to access a space or pathway of a defined Security Grade

3.1.7
cabling
system of telecommunications cables, cords and connecting hardware that supports the connection of information technology equipment
[SOURCE: ISO/IEC 11801-1:2017, 3.1.21]

3.1.8
common distribution space
primary or secondary building distribution space

3.1.9
countermeasure
step taken to prevent a threat triggering a security event

3.1.10
dialler unit
device that communicates with external monitoring or response entities to report exceptions to pre-programmed conditions via a specific telephone number, set of telephone numbers or a network connection.

3.1.11
door hardware
metallic fixtures that enable opening, closing, and locking a door

3.1.12
electronic locking mechanism
device that allows access following receipt of digital or analogue information indicating an appropriate authorisation status of the person entering the information

AVA Documents
Document Sharing Hub
Full document details: 21/30446697 DC

3.1.13
effective height of a free-standing barrier
shortest distance between any point on the top of the permanent part of the free-standing barrier (excluding any toppings) and the surface of the supporting ground when measured in the plane of the barrier

3.1.14
external boundary
physical barrier(s) demarcating a space or structure of a given Security Grade (SG)

Note 1 to entry: Access floors and suspended ceilings through which unauthorised access to a space can be gained are not considered to be external boundaries. In such cases, the fixed building fabric upon which these structures are built is the external boundary.

3.1.15
external telecommunications cabinet
outdoor enclosure accommodating telecommunications equipment and associated cabling

3.1.16
free-standing barrier
wall, fence, gate, turnstile or other similar self-supporting barrier, and its associated foundations, designed to prevent entry to a space of a given Security Grade

3.1.17
intelligent building system
equipment and telecommunication infrastructure that supports monitoring, control, operation and management of building services

3.1.18
keypad
manual input devices, typically requiring telecommunications connectivity, that allow individuals to enter specific codes to arm, disarm or diagnose intrusion systems

3.1.19
joint closures
sealed housing protecting the joining or splicing of the conductors and optical fibres of telecommunications cables

3.1.20
junction box
protective housing and associated space that enables cables to be routed between pathway systems

3.1.21
mechanical locking mechanism
device that allows access by means of physically coded key or tool

3.1.22
protected distribution system
conduit, hardened raceway, hardened optical fibre cable, and other means of physically restricting the access to telecommunications cables

3.1.23
security event
vulnerability that has been exploited by a threat

3.1.24
surveillance system
devices and mechanisms used to monitor and detect behaviour or activity to protect the physical network

3.1.25
tamper evident
designed or enabled to show access or attempts to access

AVA Documents
Document Sharing Hub

Full document details: 21/30446697 DC

3.1.26
terminal equipment
equipment at an outlet used to access information provided by transmission equipment

[SOURCE: ISO/IEC 11801-1:2017, 3.1.81]

3.1.27
terminal equipment outlet
fixed connecting device which provides an interface to the terminal equipment
[SOURCE: ISO/IEC 11801-1:2017, 3.1.80, modified - Note 1 to entry deleted]

3.1.28
threat
method by which a vulnerability can be exploited to create a security event

3.1.29
topping
construction, added to the top of a free-standing barrier, and designed to be an effective intruder deterrent or for a decorative display of security

3.1.30
transmission equipment
active equipment used to distribute information from distributors to other distributors and to outlets
[SOURCE: ISO/IEC 11801-1:2017, 3.1.84]

3.1.31
vulnerability
weakness that can be potentially exploited by a threat

3.2 Abbreviations

For the purposes of this document the abbreviations of ISO/IEC 14763-2 and the following apply.

CMS cable management system

SG Security Grade

4 Conformance

For the physical network security of a telecommunications cabling infrastructure to conform to this document it shall conform, as a minimum, to the specification, planning, installation and installation requirements of ISO/IEC 14763-2. This provides a basic level of physical network security and addresses the minimum information sensitivity level denominated Open.

In order to provide increased levels of physical network security determined by a risk assessment, the requirements for higher information sensitivity levels restricted, secure or highly secure shall be met.

Documents
Document Sharing Hub

Full document details: 21/30446697 DC

5 Principles

5.1 General

A cyber security strategy sets out an organization's guiding principles, objectives and priorities for cyber security and shall also cover an organization's threat environment, cyber security initiatives (an action plan), or investments the organization plans to make as part of its cyber security program.

Without a cyber security strategy, organizations risk failing to adequately plan for and manage security and business risks within their organization.

Organizations can protect their systems and information from cyber threats. These security principles are grouped into four key activities: govern, protect, detect and respond.

a) **Govern:** Identifying and managing security risks.

b) **Protect:** Implementing security controls to reduce security risks.

c) **Detect:** Detecting and understanding security events.

d) **Respond:** Responding to and recovering from cyber security incident.

The focus of this document assists in the effort to enhance the security, resiliency, and reliability of the organization's cybersecurity and communications infrastructure: **Protect**.

5.2 Relationship with ISO/IEC 27000 series

The ISO/IEC 27000 series is a series of 46 individual standards that assist organizations improve their cyber information security; ISMS (information security management system). The ISMS is a systematic approach to risk management, containing measures that address the three pillars of information security: people, processes and technology.

ISO/IEC 24383 provides direction on security controls and treatments around information technology cabling, pathways and spaces for customer premises. These measures are not discussed in ISO/IEC 27000 series. ISO/IEC 24383 has been prepared so that it dovetails into ISMS, addressing cyber infrastructure security, to provide organizations with a complete, effective end-to-end cyber security implementation.

5.3 Risk assessment concepts

5.3.1 General

ISO/IEC 24383 does not address risk assessment techniques or any form of analysis. The organization is responsible to determine the cyber security risks that it faces.

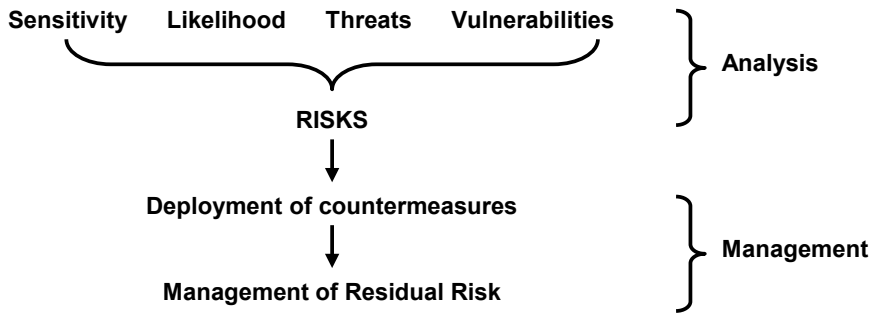

Figure 1 – Risk assessment concepts

This document nominates four levels of information sensitivity, and the controls and treatments for those nominated sensitivity levels.

The organization can determine that they require additional classifications of information sensitivity levels. These additional levels will not impact on the controls or treatments nominated in ISO/IEC 24383. The organization can expand on the treatments and controls discussed in this standard.

5.3.2 Information sensitivity levels

The four levels of information sensitivity (classification) are:

Documents
Document Sharing Hub
Full document details: 21/30446697 DC

a) Open: unauthorized disclosure, alteration or destruction of that information would result in little or no risk to the organization. This information includes, but is not limited to:

   1) Public information, and can be openly shared on your website, discussed in public and with anyone.

   2) Organization-wide internal information and should be protected with limited (cyber) controls. Internal information can include the employee handbook, various policies and organization-wide memos.

NOTE: In ISO/IEC 24383 the security treatments and controls for information technology cabling, pathways and spaces for open (cyber) classification in a “public accessible area” and an organization’s general “working” area are the same. There are many circumstances where a physical barrier does not exist. Distinction between these “open” spaces is only made when the organization is locating the equipment room and applying equipment room specific security.

[Editor’s note: Text should be included to clarify that the "open" information sensitivity level must meet the minimum installation requirements specified in ISO / IEC 14763-2]

b) Restricted: unauthorized disclosure, alteration or destruction of that information could result in a moderate level of risk to the organization. This information includes, but is not limited to:

   1) Confidential information is team-wide, and its use should be contained within the business.

   2) This information can include highly controlled pricing or contact information, sensitive HR information, or strictly confidential information could strongly-negatively affect your organization and is shared only team-wide.

c) Highly sensitive – requires a secure facility: unauthorized disclosure, alteration or destruction of that information could cause a significant level of risk to the organization. If disclosed, there would be a significant financial or legal impact to the business. This information includes, but is not limited to:

   1) Restricted information is highly sensitive, and its use should be limited on a need to-know basis.

   2) Restricted information is typically protected with a non-disclosure agreement (NDA) to minimize legal risk.

   3) Restricted information includes trade secrets, potentially identifiable information (PII), cardholder data (credit cards), or HR and health information.

d) Critically sensitive – requires a Highly secure facility: unauthorized disclosure, alteration or destruction of that information could cause a catastrophic level of risk to the organization and stakeholders / partners. This information includes, but is not limited to:

   1) Development, or likely corporate theft (nominally state-sponsored espionage) of patented technology, of significant value to an organization.

   2) Critical infrastructure command and control systems, such as energy generation plant/distribution, water and waste plant/distribution, and transportation.

5.4 Defence in depth

5.4.1 General

Defence in depth is a strategy used in Information (cyber) security in which multiple layers of security controls are layered in order to protect valuable data and information. ISO/IEC 24383 would form part of a larger ISMS (ISO/IEC 27000 series) cyber security defence in depth strategy.

ISO/IEC 24383 takes a systematic approach when applying security treatments and control to information technology cabling, pathways and spaces for customer premises. The defence in depth is a strategy undertaken is as follows:

a) Public perimeter,

b) Organizational perimeter,

c) Equipment/distributor room,

Documents
Document Sharing Hub

Full document details: 21/30446697 DC

d) Rack/cabinet,

e) Cabling component containment,

f) Cabling component.

The application of defence-in-depth for the protection of IT cabling systems and the cyber information moving across the IT cabling, is enhanced using successive layers of physical security. All layers are designed to limit access to people without the appropriate authorisation to access systems at a facility.

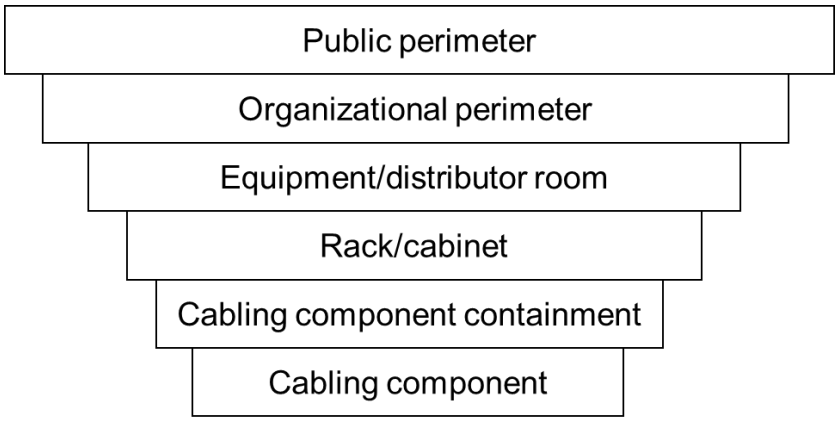

Figure 2 – Defence in depth model

5.4.2 Public perimeter

The first layer in the protection of information technology cabling, pathways and spaces is the line demarcating the boundary between the public accessible areas and the organizational side.

The line demarcating the extent between the public accessible areas and the organizational side is often a physical barrier (visible or non-visible). This physical barrier is dependent on the organization and the facility. This demarcation could be:

a) Buried sensing cables and motion detectors around the site.

b) A security rated fence and commensurately rated portals around the site.

c) Access control doors (mechanical or electronic) from a public foyer or waiting area.

d) Access control doors (mechanical or electronic) from a public open area (e.g. parks, gardens, and the like).

Access points within the demarcation line provides a means of organization personnel (people or vehicles) on entering/exiting between public area and the organization area.

5.4.3 Organizational perimeter

The second layer in the protection of information technology cabling, pathways and spaces is the line demarcation between the internal boundary between the various classified areas within the organization facility. These various classified areas can be:

a) Open,

b) Restricted,

c) Secure,

d) Highly secure.

Only the (cyber) information of that classification or lower, can be created, disclosed, altered or destroyed in that classification of area.

AVA Documents
Document Sharing Hub

Full document details: 21/30446697 DC

As an example, Restricted Network (RN) telecommunications outlets and workstations can appear in the Restricted Area (RA) and in the Secure Area (SA). Secure Area (SA) telecommunications outlets and workstations are prohibited to appear in either the Restricted Area (RA) or the Open Area (OA).

It is feasible for an organization two have two separate Restricted networks, each one existing solely and independently within a restricted area. As an example, Restricted Network 1 (RN1) can only have telecommunications outlets and workstations in Restricted Area 1 (RA1); likewise, Restricted Network 2 (RN2) telecommunications outlets and workstations can only appear Restricted Area 2 (RA2) and are prohibited in Restricted Area 1 (RA1), and vice versa.

5.4.4 Equipment/distributor room

The third layer in the protection of information technology cabling, pathways and spaces systems is the equipment rooms and distributor rooms. Within ISO/IEC 24383 all these rooms and spaces will be referred as the Equipment/distributor room (ER).

The security treatments and access for the equipment room housing the various classified (open, restricted, secure, highly secure) network cabling and/or equipment will differ.

The equipment room shall be classified to the highest level of the network rack/cabinet present in the room. There is a solution for the facility that houses a HSER, without a secure area. This is not recommended and is the only solution of existing facilities, with limited capability to be upgraded only.

After the equipment room has been classified, the equipment room shall be located in an area that is at a maximum of one classification level less than the equipment room. Where equipment rooms are placed in an area that is at a lower classification than the equipment room, additional security treatments shall be applied.

Table 1 – Equipment room classification and minimum area classification

Network rack/cabinet present	Equipment room classification	Minimum area classification
Open network (ON)	Open ER (OER)	Open area (public space)
Restricted network (RN)	Restricted ER (RER)	Open area (organization space)
Secure network (SN)	Secure ER (SER)	Restricted area
Highly secure network (HSN)	Highly secure ER (HSER)	Restricted Area (Secure area recommended)

5.4.5 Rack/cabinet

The fourth layer in the protection of information technology cabling, pathways and spaces systems is the equipment rack/cabinet.

The equipment rack shall be classified to the highest level of the (classified) network present in the rack/cabinet.

The security treatments and access for the equipment racks/cabinets that are classified either open, restricted, secure, highly secure will differ.

5.4.6 Cabling component containment

The fifth layer in the protection of information technology cabling, pathways and spaces systems is cabling component containment.

Documents
Document Sharing Hub
Full document details: 21/30446697 DC

The cabling containment and the associated security treatments and controls shall match the classification of the network (information technology) cabling within.

5.4.7 Cabling component

The sixth layer in the protection of information technology cabling, pathways and spaces systems is the cabling component (cable, cord or connecting hardware).

The security treatments and controls for the cable, cords and outlets and the like shall match the classification of the network (information technology) information that is being transported over the cabling component.

5.5 Network infrastructure

While physical security can provide a degree of protection to information communicated over network infrastructure. Organizations can increase control over cyber-information when it is communicated over network infrastructure; it is recommended that all the network and cabling infrastructure is located in the areas authorised for the processing of such cyber-information.

5.6 Controlling access

Physical security controls are implemented to protect network devices and cabling, especially those in public areas, from physical damage or unauthorised access.

Risk assessed physical protection shall be provided for all network devices and cabling, especially those in public areas, to prevent an adversary physically damaging a network device with the intention of interrupting services. The physical protection shall be fit for the intended purpose.

Physical access to network devices can allow an adversary to reset devices to factory default settings by pressing a physical reset button, connecting a serial interface to a device or connecting directly to a device to bypass any access controls.

Resetting a network device to factory default settings can:

a) Disable security settings including authentication and encryption functions.

b) Reset administrator accounts and passwords to known defaults.

c) If access to a network device is not gained, a likely denial of service attack could occur.

Physical access to network devices can be restricted through methods such as physical enclosures that prevent:

1) Access to console ports and factory reset buttons.

2) Mounting devices on ceilings or behind walls.

3) Placing devices in locked rooms or cabinets.

Physical access to cabling can allow threats to tap cables to obtain the information being transmitted and to insert signals to manipulate network components.

5.7 Perimeters and spaces

5.7.1 General

This clause discusses the relationship between areas of various classifications, and equipment rooms of various classifications. This clause outlines the requirements and recommendations for perimeter security and access control at the demarcation line between the internal boundary between the various classified areas within the organization facility.

Documents
Document Sharing Hub

Full document details: 21/30446697 DC

5.7.2 Area and room relationships

5.7.2.1 General

The location of the various classified areas and equipment rooms will differ from organization to organization. Even within an organization, the purpose and layout of facilities will differ.

Figure 3, Figure 4 and Figure 5 do not encompass all cyber infrastructure classification installation solutions. Their purpose is to demonstrate the relationship and logic on the placement of:

a) Areas of various classification that house telecommunications outlets and workstations.

b) Placement of equipment rooms of various classifications.

5.7.2.2 Example: solution one

In this example there are four separate classified areas; open, restricted, secure and highly secure. The information technology security philosophy behind the example in Figure 3 is as follows:

a) In the open area, “Open network (ON)” telecommunications outlets and workstations are located.

b) In the restricted area, “Open network (ON)” and “Restricted network (RN)” telecommunications outlets and workstations are located. There are two separate equipment room; Open ER (OER) and a Restricted ER (RER).

c) In the secure area, “Open network (ON)”, “Restricted network (RN)” and “Secure network (SN)” telecommunications outlets and workstations are located. There is one separate equipment room; Secure ER (SER).

d) In the highly secure area, “Open network (ON)”, “Restricted network (RN)”, “Secure network (SN)”and “Highly secure network (HSN)” telecommunications outlets and workstations are located. There is one separate equipment room; Highly secure ER (HSER).

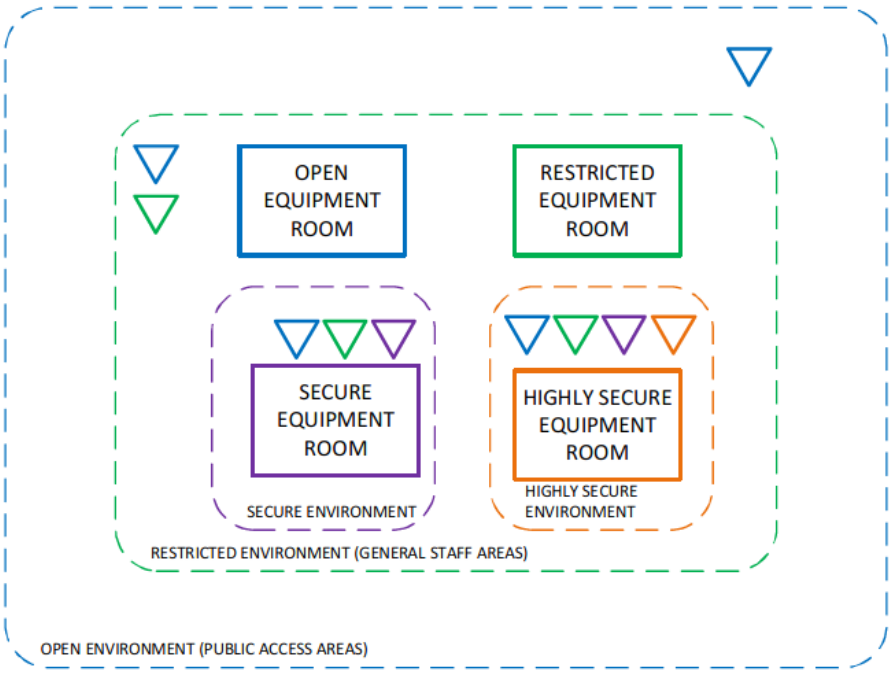

Figure 3 – Area and room relationship – solution one

Documents
Document Sharing Hub
Full document details: 21/30446697 DC

5.7.2.3 Example: solution two

In this example there are four separate classified areas; open, restricted, secure and highly secure. The information technology security philosophy behind the example in Figure 4 is as follows:

a) In the open area “Open network (ON)” telecommunications outlets and workstations are located. In this situation, the organizational “Open ER (OER)” is directly accessible from a public space. This OER will require additional security treatments and controls equivalent to a Restricted ER (RER). Due to the location “Restricted network (RN)”, “Secure network (SN)”and “Highly secure network (HSN)” racks/cubicles are prohibited.

NOTE: In this situation, a Restricted area was built around the OER.

b) In the restricted area, “Open network (ON)” and “Restricted network (RN)” telecommunications outlets and workstations are located. There are two separate equipment room; a Restricted ER (RER) and a Secure ER (SER). The Restricted ER needs additional treatments.

c) In the secure area, “Open network (ON)”, “Restricted network (RN)” and “Secure network (SN)” telecommunications outlets and workstations are located. There is one separate equipment room; Highly secure ER (HSER). The Highly Secure ER needs additional treatments.

d) In the highly secure area, “Open network (ON)”, “Restricted network (RN)”, “Secure network (SN)”and “Highly secure network (HSN)” telecommunications outlets and workstations are located.

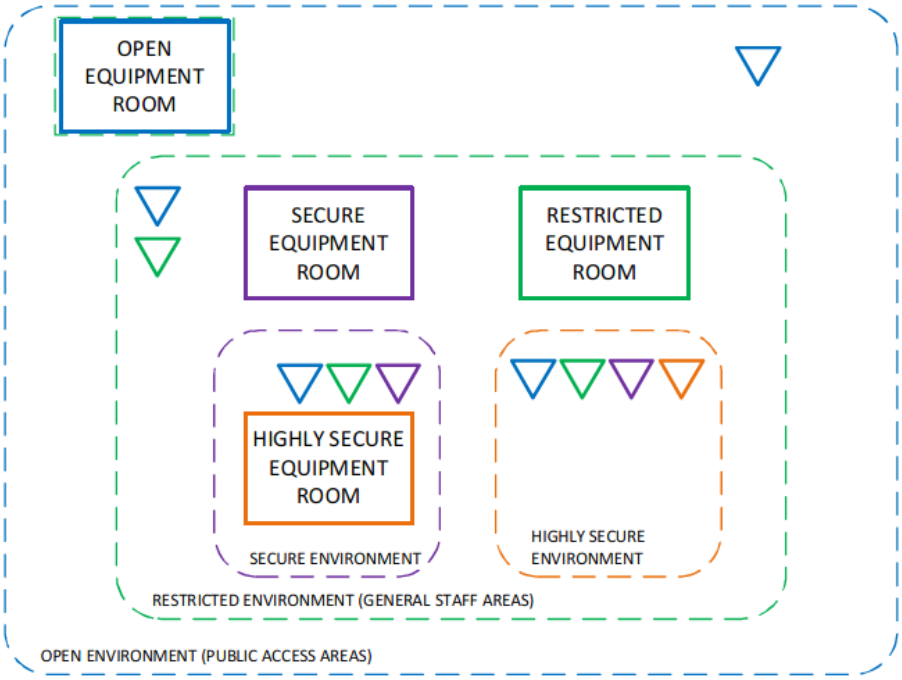

Figure 4 – Area and room relationship – solution two

5.7.2.4 Example: solution three

In this example there are four separate classified areas; open, restricted, secure and highly secure. The information technology security philosophy behind the example in Figure 5 is as follows:

a) In the open area “Open network (ON)” telecommunications outlets and workstations are located. In this situation, the organizational “Open ER (OER)” is directly accessible from a public space. This OER will require additional security treatments and controls equivalent

AVA Documents Document Sharing Hub
Full document details: 21/30446697 DC

to a Restricted ER (RER). Due to the location “Restricted network (RN)”, “Secure network (SN)”and “Highly secure network (HSN)” racks/cubicles are prohibited.

NOTE: In this situation, a Restricted area was built around the OER.

b) In the restricted area, “Open network (ON)” and “Restricted network (RN)” telecommunications outlets and workstations are located. Due to constrains, there are three separate equipment rooms; a Restricted ER (RER), a Secure ER (SER) and a Highly secure ER (HSER). The SER and HSER will require additional security treatments and controls equivalent to a Secure ER (RER) – in essence, a secure area is being built around the HSER to bring it into line with the recommendations of Table 1. This is absolutely the lowest classified area that a HSER shall be found.

c) In the secure area, “Open network (ON)”, “Restricted network (RN)” and “Secure network (SN)” telecommunications outlets and workstations are located.

d) In the highly secure area, “Open network (ON)”, “Restricted network (RN)”, “Secure network (SN)”and “Highly secure network (HSN)” telecommunications outlets and workstations are located.

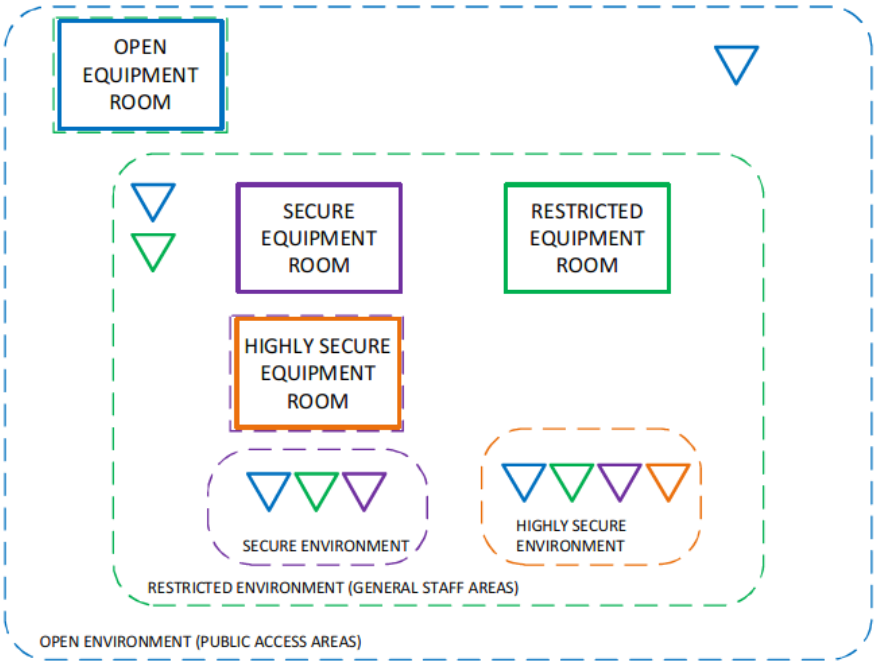

Figure 5 – Area and room relationship – solution three

5.7.3 Unauthorized observation

The inside of facilities without sufficient perimeter security are often exposed to observation through windows by unauthorized people.

Ensuring systems and information are not visible through windows will assist in reducing this security risk. This can be achieved by using blinds or curtains on windows. Soft or non-resonating window covering can prevent laser monitoring.

5.7.4 Security treatments and controls

The purpose of the security treatment and controls is to:

a) Control and restrict access to various classified telecommunications outlets and workstations.

b) Control and restrict access to various classified networks.

Documents
Document Sharing Hub
Full document details: 21/30446697 DC

c) Provide a demarcation line between the internal boundary between the various classified areas within the organization facility.

These required security treatment and controls shall apply these principles:

1) Deter – ensure that significant difficulty for adversaries to defeat, based on the classification.

2) Detect – identify unauthorised actions to gain access.

3) Delay – impede an adversary during attempted entry.

4) Respond – resist or mitigate the attack or event when it is detected.

5) Recover – restore operations to normal levels following an event.

All these area layers are designed to limit access to people without the appropriate authorisation to access systems at a facility.

5.8 Threat

Although risk is mostly defined by security classification level, area construction and protection measures will vary by and need to conform to the threat for the specific location. A low threat location (host country government compound, military base, etc.) should have lower protection requirements than a high threat location (commercial building in adversary country, etc.). The threat level shall be determined prior to selection of protection criteria.

6 Public perimeter

[Editor's note: The sub-clauses corresponding to requirements and recommendations that have no content, remain as "place-holders" until the completion of the CD stage. At the end of this stage, any requirement or recommendation subclause that remains empty will be removed. The requirements or recommendations subclauses corresponding to the "open" information sensitivity level will generally be empty, unless a requirement or recommendation not specified in ISO/IEC 14763-2 is specified. For which, its inclusion in the living list should also be considered for future revisions of said standard]

6.1 Spaces and structures

6.1.1 Access control

6.1.1.1 Requirements

6.1.1.1.1 Open

Closable and lockable entry doors are required.

6.1.1.1.2 Restricted

6.1.1.1.3 Secure

6.1.1.1.4 Highly secure

6.1.1.2 Recommendations

6.1.1.2.1 Open

6.1.1.2.2 Restricted

6.1.1.2.3 Secure

Pubic perimeter for secure facilities should have fencing at the boundary or the outside area with lockable gates for after-hours use.

6.1.1.2.4 Highly secure

Pubic perimeter for highly secure facilities should have fencing at the boundary or the outside area with lockable gates for after-hours use. Perimeter lighting and CCTV monitoring to a security position or facility, or periodic guard patrols should be considered.

AVA Documents
Document Sharing Hub

Full document details: 21/30446697 DC